

## Handout 11: Cool Irreducibility Tests

Here are three cool tests for irreducibility, two of which you'll prove in class today:

1. **Gauss's Theorem (3.96).** Let  $f(x) \in \mathbb{Z}[x]$ . If  $f(x)$  factors as  $G(x)H(x)$  in  $\mathbb{Q}[x]$ , then it also factors as  $f(x) = g(x)h(x)$  in  $\mathbb{Z}[x]$ , where  $\deg(g) = \deg(G)$  and  $\deg(h) = \deg(H)$ . Therefore, if  $f$  does not factor into polynomials of smaller degree over  $\mathbb{Z}$ , it is irreducible in  $\mathbb{Q}[x]$ .
2. **Theorem (3.97).** Let  $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$  be a monic polynomial in  $\mathbb{Z}[x]$ , and let  $p$  be prime. Let  $f^*$  be obtained from  $f$  by reducing its coefficients modulo  $p$ . Then if  $f^*$  is irreducible in  $\mathbb{Z}_p[x]$ ,  $f$  is irreducible in  $\mathbb{Q}[x]$ .

*Proof.* Note that  $f^*$  is the image of  $f$  under the homomorphism  $\phi^* : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$  that reduces coefficients modulo  $p$ .

What happens if  $f$  factors as  $g \cdot h$  in  $\mathbb{Z}[x]$ , where both  $g$  and  $h$  have smaller degree than  $\deg(f)$ ?

What does  $f$ 's monicity say about  $f^*$ ? And what does this say about the degrees of  $f$  and  $f^*$ ?

Finally, note that this contradicts the irreducibility of  $f^*$  in  $\mathbb{Z}_p[x]$ , since an earlier proposition (3.64) now implies  $f^*$  is *not* irreducible.

Now what does Gauss's Theorem say?

To paraphrase this last result, we can say "irreducible over  $\mathbb{Z}_p$  implies irreducible over  $\mathbb{Q}$ ." Note, however, that this gives a *powerful* tool for testing irreducibility in  $\mathbb{Q}$ , since in  $\mathbb{Z}_p$  there are only finitely many polynomials of a given degree, so we can test all possible factorizations if we're patient enough!

**Example.** Is  $f(x) = x^3 - x - 7$  irreducible in  $\mathbb{Q}[x]$ ?

**Example.** Is  $g(x) = x^3 + 9x^2 + 5x + 1$  irreducible in  $\mathbb{Q}[x]$ ?

3. **Eisenstein's Criterion.** If  $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$  and there is a prime  $p$  dividing  $a_i$  for all  $i < n$  but  $p \nmid a_n$  and  $p^2 \nmid a_0$ , then  $f$  is irreducible in  $\mathbb{Q}[x]$ .

**Example.** Is the polynomial  $f(x) = 48x^4 + 28x^3 - 42x^2 + 21x + 126$  irreducible in  $\mathbb{Q}[x]$ ?

**Example.** How about  $g(x) = x^3 - 42x^2 + 21x + 127$ ?

**Homework.** The following problems are due *Friday, February 27th*, at 5:00 p.m.:

1. Do exercise 3.86 from your text.
2. Do exercise 3.87 from your text.
3. Come up with a polynomial for which Theorem 3.97 can be used to prove irreducibility with  $p = 3$ , but for which the same theorem does not yield any information with  $p = 2$ . (Your polynomial should differ from the example given above!)
4. Come up with a polynomial for which Theorem 3.97 can be used to prove irreducibility with  $p = 5$ , but for which the same theorem does not yield any information with either  $p = 2$  or  $p = 3$ .
5. Come up with a polynomial for which Theorem 3.97 can be used to prove irreducibility with  $p = 7$ , but for which the same theorem does not yield any information with any of  $p = 2$ ,  $p = 3$ , or  $p = 5$ . Can you see how to generalize your construction?

Problems 3, 4, and 5 will be “modified” committee problems: on Wednesday those of you who have completed these problems will be asked to share your polynomials with the rest of the class, and we will discuss all submissions as a class.